RIGHT TO PRIVACY IN CYBERSPACE: A CRITICAL STUDY

PhD SYNOPSIS

Supervisor:
Prof. (Dr.) Nishtha Jaswal,
Vice-Chancellor,
Himachal Pradesh National Law University,
Shimla, Himachal Pradesh.

Submitted By:
Anshul Singhal,
Ph.D. Scholar,
Himachal Pradesh National Law University,
Shimla, Himachal Pradesh.
Enrolment No. 9020212201

RIGHT TO PRIVACY IN CYBERSPACE: A CRITICAL STUDY

INTRODUCTION

It is a settled position that the individual is the focal point of the Constitution. It cannot be lost sight of that it is in the realisation of individual rights that the collective well-being of the community is determined. An individual has been given several rights under the Indian Constitution which are contained under Part-III (Articles 12 to 35) and are known as the "Fundamental Rights". Fundamental Rights are considered essential for the development of the personality of every individual and to preserve human dignity. Broadly stated, the Fundamental Rights as contained in Part-III of the Indian Constitution are Right to Equality, Right to Freedom, Right against exploitation, Right to Freedom of Religion, Cultural and Educational Rights and Right to Constitutional Remedies.

Of all the fundamental rights enshrined in the Indian Constitution, Article 21 is considered to be the heart of the Constitution. Article 21 deals with the Protection of Life and Personal Liberty and states that, 'No person shall be deprived of his life or personal liberty except according to procedure established by law.'[1] Article 21 encompasses several inviolable rights available to the individuals. The scope of article 21 has been widened from time to time by Hon'ble Supreme Court of India and various High Courts to ensure that right to life means a dignified life. One of the facet of right of life and personal liberty as enshrined under article 21 of the Indian Constitution is the right to privacy of an individual.

Vide Article 12 of the Universal Declaration of Human Rights, the right to privacy has been recognised as a basic human right. Article 12 of UDHR states that, 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.[2] Article 17 of the International Covenant on Civil and Political Rights though very similarly worded as Article 12 of UDHR, declares the right to Privacy to be an important civil and political right and states that, 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.'[3] It further states that, 'Everyone has the right to the protection of the law against such interference or attacks'[4].

1 The Constitution of India, 1950, A. 21.
2 Universal Declaration of Human Rights, 1948, A. 12.
3 International Covenant on Civil and Political Rights, 1966, A. 17(1).
4 *Id.,* A. 17(2).

The right to privacy is a basic, natural, primordial, inalienable and inherent right of a human. Privacy constitutes the foundation of all liberty. Without the right to privacy, a person cannot enjoy his liberty and dignity. Furthermore, the right to privacy enables individual autonomy and ensures the exercise and enjoyment of liberty and freedoms. However, it would not be false to state that liberty has a broader meaning of which privacy is a subset. Liberty is essential for the meaningful human existence. The contours of privacy have been beautifully explained by Geoffrey Fischer, who was an English Anglican priest, and 99th Archbishop of Canterbury, serving from 1945 to 1961, in the following words:

> 'There is a sacred realm of privacy for every man and woman where he makes his choices and decisions-a realm of his own essential rights and liberties into which the law, generally speaking, must not intrude.'[5]

We can gather two things from the wise words of Mr. Geoffrey Fischer, first, that everyone should enjoy their right to privacy and second, that the right to privacy granted to every person is not absolute. To put it in crude terms, privacy is a right of the person to be left alone. The right to privacy derives from an individual right to his or her own life, liberty, property and pursuit of happiness. The Concept and definition of the privacy has been changed during the time affecting by different factors. At the same time, the boundaries of privacy may differ from one place to another affecting by the culture, religion, etc.[6] It is very difficult to define privacy. Many jurists have made an attempt at improving the overall understanding of the concept of privacy. There are mainly two approaches to the definition of privacy. One is the unitary conception of privacy in the form of unitary conceptual core and the other is the pluralist concept of privacy wherein privacy is deemed to be consisting of several sub-types. The unitary concept focuses on the value of privacy and the understands the concept of privacy as a whole. On the other hand, under the typological approach, the theorists focus on the rights that are actually protected under the law of the land.

It is pertinent to understand the right to privacy as it exists in India. Until recently, right to privacy was not recognised as a fundamental right under the Indian Constitution. It has not been explicitly mentioned in the Constitution and the Supreme Court has time and again refused to read the same as part of the right to life and personal liberty under article 21

5 Himakriti R and Malan N, *Right to Privacy and Data Defence*, Vol. 4, No. 5 IJMLH 1529 *available at:* https://www.ijlmh.com/paper/right-to-privacy-and-data-defence/# (last visited on Oct. 03, 2022).

6 Ali Alibeigi, Abu Bakar Munir and Md. Ershadul Karim, *Right to Privacy, a Complicated Concept to Review*, LIBRARY PHILOSOPHY AND PRACTICE (e-journal), available at: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=6272&context=libphilprac (last visited on Sept. 13, 2021).

and right to freedom of speech and expression under article 19(1)(a).[7] Though being an invaluable right, the same was not recognised.

A retired High Court Judge, J. KS Puttaswamy in 2012 had challenged the government's Aadhaar scheme which the government proposed making mandatory for access to government services and benefits. The scheme was challenged on the basis that it violated the right to privacy of the citizens. On August 11th 2015, a Bench of three judges comprising Justices Chelameswar, Bobde, and C. Nagappan passed an order that a Bench of appropriate strength must examine the correctness of the decisions in M P Sharma v Satish Chandra, District Magistrate, Delhi, 1954 (Eight Judge Bench) and Kharak Singh v State of Uttar Pradesh, 1964 (Six Judge Bench) and in particular, it ordered that the Court must decide whether we have a fundamental right to privacy.[8] This matter was first placed before a Five Judge Bench headed by the then Chief Justice Khehar. Subsequently, the matter was referred to a Nine Judge Bench on July 18th 2017. The Bench comprised Chief Justice Khehar and Justices Jasti Chelameshwar, S.A. Bobde, DY Chandrachud, Abdul Nazeer, Nariman, R.K. Agarwal, Abhay Manohar Sapre, and Sanjay Kishan Kaul.[9] The questions of reference before the bench were as follows:

(i) Whether there is any fundamental right of privacy under the Constitution and if so, where is it located and what are its contours?

(ii) What is the ratio decidendi of MP Sharma and Kharak Singh cases and whether those cases rightly decided?

The 9 judges bench of the Hon'ble Supreme Court of India discussed the international law on this point, the law as prevailing in other countries, answered the above reference in *KS Puttaswamy* v. *Union of India*,[10] as follows:

> '652.1. The decision in M.P. Sharma [M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 : 1954 Cri LJ 865 : 1954 SCR 1077] which holds that the right to privacy is not protected by the Constitution stands overruled;
> 652.2. The decision in Kharak Singh [Kharak Singh v. State of U.P., AIR 1963 SC 1295 : (1963) 2 Cri LJ 329 : (1964) 1 SCR 332] to the

7 *See MP Sharma* v. *Satish Chandra*, AIR 1954 SC 300 (8 Judges Bench) and *Kharak Singh* v. *State of UP*, AIR 1963 SC 1295 (6 Judges Bench).

8 SUPREME COURT OBSERVER, *Fundamental Right to Privacy, available at:* https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/amp/ (last visited on Oct. 03, 2022).

9 *Ibid.*

10 *KS Puttaswamy* v. *Union of India*, (2017) 10 SCC 1.

> extent that it holds that the right to privacy is not protected by the Constitution stands overruled;
> 652.3. The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.'[11]

It has also been held in the judgement itself that right to privacy is subject to restrictions and is not an absolute right. However, it has been further held that any such restrictions on the right to privacy should withstand the test of reasonable restrictions in article 19(2) and permissible restrictions under article 21. It has been further held that an invasion of life or personal liberty must meet the following[12]:

(i) legality, which postulates the existence of law;

(ii) need, defined in terms of legitimate state aim; and

(iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

Any violation of right to privacy should be, firstly, sanctioned by law, secondly, must be necessary in a democratic society for a legitimate aim, thirdly, the test of proportionality should be applied and the violation should be in direct consonance with the objective sought to be achieved and lastly, there must be procedural guarantees against abuse of such interference.[13] The nature and quality of encroachment on a right should not be disproportionate to the purpose to be achieved by such law and this test of proportionality guards against arbitrary state action and protects the Fundamental Rights of individuals. The Hon'ble Court recognised certain other rights as well which emanate from the right to privacy particularly in cyberspace, internet, social media, etc. which are as follows[14]:

(i) Right to identity.

(ii) Right to control dissemination of personal information.

(iii) Right to be forgotten.

The court further held that mere absence of express enumeration of the right to privacy under the Indian Constitution is no ground for disregarding its omnipresence in Part III. In other words, the absence of an express constitutional guarantee of privacy does not necessarily warrant that there is no protection of privacy under the framework of protected

11 *Id.,* para 652.
12 *Id.,* para 325.
13 *Id.,* para 638.
14 *Id.,* per Justice Sanjay Kishan Kaul.

guarantees including those in Article 19 and 21.[15] The Hon'ble court went even to the extent to hold that right to privacy cannot be denied even if only a minuscule fraction of the society or the country's population is being affected by the violation of such a right.

The umbrella term privacy itself encompasses both the concept of what privacy is and how it should be valued as well as a (generally) narrower right to privacy outlining the extent to which privacy is or ought to be legally protected.[16] The German Constitutional Court even went to the extent of protecting the right to confidentiality and integrity of computer systems as a part of right to privacy. The unlawful access to computer systems has been criminalised in Italy. The protection of computer systems emerges from the concept of inviolability of the home. The US Supreme Court while upholding the right to privacy as per the fourth amendment of the US Constitution has held that the police needs to obtain a warrant even for searching a seized cellphone while making an arrest.[17]

The above protections have been given as computers and cell phones are the new 'place' where information related to the life of a person is stored. In India, however, only when a computer system is declared a protected system under the Information Technology Act, 2000, can such a system enjoy the protections that are generally available in other democratic countries of the world. A government can also declare a computer, computer system or network as a protected system if it feels, at any point of time, that it is critical for public interest and that any compromise with regard to its security could impact people, groups or even the society.[18]

Thus, in India, the confidentiality and the integrity of the computer system is protected only when it is in the interest of the general public and an individual has no such right. Hence, an individual is prone to cyber attacks and there is a need to provide for adequate cybersecurity to individuals as well.

Informational privacy reflects an interest in preventing information about the self from being disseminated, and controlling the extent of access to information. The Court thus recognised information privacy as a facet of the right to privacy and recommended that the Government of India should examine and put in place a robust mechanism for data

15 Nidhi Singh, *Defining the Right to Privacy in India in light of Justice KS Puttaswamy & Anr. v. Union of India*, OXHRH BLOG, 5 October 2017, *available at:* https://ohrh.law.ox.ac.uk/defining-the-right-to-privacy-in-india-in-light-of-justice-ks-puttaswamy-anr-v-union-of-india-2017 (Last Visited on Sept. 21, 2022).

16 Bert-Jaap Koops, Bryce Clayton Newell, et. al., *A Typology of Privacy*, 38:2 U. PA. J. INT'L L. 491 (2017).

17 *Riley* v. *California*, 573 U.S. 373 (2014).

18 Pavan Duggal, *Protected Systems and Networks*, THE ECONOMIC TIMES [E-PAPER (ENGLISH EDITION)], Last Updated Apr. 13, 2003, *available at:* https://economictimes.indiatimes.com/protected-systems-and-networks/articleshow/43196757.cms (Last Visited on Sept. 21, 2022).

protection. This exercise is quite tricky because it would require a fair balance between the rights of citizens and state.[19]

Privacy has several aspects, such as, privacy in personal life, privacy of information, privacy in cyberspace, etc. For the purposes of this study, the researcher will focus only on right to privacy in cyberspace and the major privacy concerns that arise in cyberspace.

Before moving forward, it is pertinent to understand the meaning of cyberspace. The generally accepted definition is that 'Cyberspace is the notional environment in which communication over computer networks occurs.' However, the National Cyber Security Policy, 2013 has defined cyberspace more elaborately in the following words:

> 'Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.'[20]

Protection of personal data against violation by other individuals as well as the corporate is an important facet of privacy in cyberspace. The European Union has notified the General Data Protection Regulations (GDPR) which protects the personal data (information) of the individuals. Pursuant to this, in India, Justice Sri Krishna Committee was set up to look into the matter of protection of data of the individuals. Taking into account the recommendations of the committee, the Data Protection Bill was introduced in the Parliament. However, because it could become the law of the land, the Centre on August 03, 2022 withdrew the controversy-ridden Personal Data Protection Bill, 2021 and said it would soon be replaced by "a comprehensive legal framework," that will be "designed to address all of the contemporary and future challenges of the digital ecosystem,".[21]

Another important facet of privacy in cyberspace is providing cyber security. With the objective of combating cyber attacks and providing cyber security, the Government introduced the National Cyber Security Policy, 2013. The National Cyber Security Policy of India aims at fortification of information infrastructure in cyberspace, counter cyber hazards and diminish injuries from cyber incidents through an amalgamation of institutional

---

19 Nidhi Singh, *Defining the Right to Privacy in India in light of Justice KS Puttaswamy & Anr. v. Union of India*, OXHRH BLOG, 5 October 2017, *available at:* https://ohrh.law.ox.ac.uk/defining-the-right-to-privacy-in-india-in-light-of-justice-ks-puttaswamy-anr-v-union-of-india-2017 (Last Visited on Sept. 21, 2022).

20 National Cyber Security Policy, 2013, Point 1 of the Preamble.

21 THE ECONOMIC TIMES, *Govt withdraws data protection bill, 2021, available at:* https://economictimes.indiatimes.com/tech/technology/govt-withdraws-data-protection-bill-2021/articleshow/93334281.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last visited on Oct. 04, 2022).

organisations, individuals, method, technology and assistance. The main purpose is to build a secure cyberspace and reinforce the regulatory structure. Several strategies under different heads have been formulated by the Government under this policy to combat cyber crimes.

The study will discuss the concept and origins of right to privacy, the current legal framework and the provisions pertaining to privacy in cyberspace in other jurisdictions of the world. This study will also focus on the major privacy concerns in cyberspace such as protection of data, cyber security, digital surveillance, etc.

STATEMENT OF PROBLEM

Right to privacy has been held to be both a common law right as well as a fundamental right. In case of violation of right to privacy by non-state actors, an action would lie under the common law and in case of violation of right to privacy by the State itself, then an action would lie for violating the Fundamental Right to privacy under Article 32 of the Indian Constitution. As has already been discussed, right to privacy has several different facets, one of them being, the right to privacy in cyberspace. Ours is an age of information and information is knowledge.

The first privacy concern is in respect of the privacy of data, or in other words, data protection. The underlying principle for the protection of data of the individuals is that every individual should have a right to be able to exercise control over his/her own life and image as portrayed to the world and to control the commercial use of his/her identity. By way of several technological advancements, it has become possible to enter a citizen's house without even knocking at his/her door and this is equally possible by both state and non-state actors. Today data is ubiquitous and whoever possesses the data possesses all the power and authority. Digital communications technologies have become part of everyday life. There has been large number of cases alleging the violation of privacy which has further increased because of modern technology and investigative journalism. There are several issues that arise pertaining to the enjoyment of the right to privacy in cyberspace. Every transaction of the individual and every site he visits leaves electronic tracks. These electronic tracks contain powerful means of information which provide knowledge of the sort of person that user is and about his interests. This has resulted in complex issues in respect of informational privacy. When compared to several other jurisdictions of the world such as the European Union and the United States of America, our nation does not have proper safeguards in place

to combat the vices and protect the data of the citizens from several non-state actors neither do we have a law in place providing data protection.

The second privacy concern is cybersecurity against cyber crimes. Where cyberspace has helped millions of people to interact and connect with each other, it has also been a source for various cyber crimes. The incidents of cyber attack have increased significantly. The number of internet users are increasing rapidly and along with this, cyber offences such as phishing, hacking, malware, terrorism with the help of cyberspace, etc., are increasing multifold and many people are falling prey to these attacks. In these circumstances, there has been a growing demand for the government to step in and monitor the situation closely and protect its citizens against such vicious attacks. Not only private individuals, but the government is also not immune to these cyber attacks. Cybersecurity has become a concern for the government, private corporations and the individuals. It has become a threat to the society as a whole.

The third privacy concern is unauthorised digital surveillance. There is a rising concern in the nation that the data that has been collected by the Government is being used for extraneous purposes and not for the legitimate purposes for which it was actually collected. This has raised various privacy concerns. The Government has not come forward to address these concerns. Rather it has maintained the stance that digital platforms are a vital tool of ensuring good governance in a social welfare State. The main concern is not with the surveillance for providing cybersecurity, storage and analysis of data so that better services may be provided but with the unauthorised and unapproved use of it which results in the violation of right to privacy of the individuals.

There are several other privacy issues that arise in the cyberspace but all of them emanate from the three major concerns as enunciated hereinbefore. The advancement of technology has raised concerns among netizens in respect to their right to be forgotten.

The right to privacy has been recognised as a part and parcel of the right to life and personal liberty enshrined under Article 21 of the Indian Constitution. Unlike some other rights, the right to privacy has not been recognised separately in the Indian Constitution. This has resulted in limiting the contours of the right to privacy. Moreover, due to lack of adequate legislation and proper executive policy, individuals' data is threatened, there is a lack of cyber security and there is no protection against unauthorised surveillance.

OBJECTIVES OF THE STUDY

The researcher has embarked on a study of the right to privacy in its relation to cyberspace. The various objectives of the study will be as follows:

1. To study the right of privacy in the context of cyber space.
2. To do a comparative study of the issue of right to privacy in cyber space with USA and UK.
3. To examine the current legal regime in respect of cybersecurity and data protection laws in the country.
4. To examine loopholes, if any in the current legal regime and giving suggestions to make it a more robust system.
5. To analyse how the right to privacy is being violated in the cyberspace by various stakeholders including the Government, the private bodies such as Google, Apple, social media, network operators, etc.

RESEARCH HYPOTHESES

1. The current legal regime in the form of the National Cyber Security Policy 2013, is not sufficient for the cyber safety concerns of the individuals, the government and also the private corporations and for controlling cyber crime.
2. The current legal regime relating to Data Protection is not appropriate to protect the private information of the people.

SIGNIFICANCE OF THE STUDY

Today, we are standing at the face of cyber warfare. Since it transcends the physical boundaries, the element of surprise, shock and confusion is laced in each cyber attack and they usually come unanticipated. War is always bad but it's going to become worse. The future wars, unlike those in the past, where a nation's armoury, fleet of ships and planes determined the outcome, are going to be cyber warfares, thus, transcending the physical boundaries of different jurisdictions.

The experts have been raising the danger alarms for the past one decade. However, the pace of the implementation of cybersecurity measures is extremely slow. In case of cyber crimes, the enormity, the suddenness and the anonymity of the attacker makes the cyber attacks all the more concerning and threatening.

Apart from cybercrime, threat to data security cannot be neglected for too long. The policymakers cannot assume that as long as the bank accounts and home internet are password protected, our national security infrastructure will remain guarded and uncompromised. This is simply not the case. A password does not protect a document. In today's era, an individual interacts and exchanges colossal amounts of data on a day to day basis. The enormity of the threat can be understood from the instance that a single snooping scam holds in it the potential to bring an individual from riches to rags.

With the advent of technology where the money transfer involving millions is just one click away and the push for Digital India, if cyber security is not increased and cybercrime is not thwarted well in time, it is going to be an utmost fiasco and may even be a threat to law and order situation where even keeping money in the banks would lose its credibility.

The present research proposes the need to not only have a robust system in place but also an imminent need to impart cyber education and requiring all the stakeholders involved in it to be vigilant. In order to cope with the rising concerns of cyber security and data protection, we need to not only be defensive in cyberspace but also our country should start investing in offensive cyber capabilities such as drones, stealth technology, Artificial Intelligence, etc.

Though there is existing research on the right to privacy and though some studies have been undertaken in the USA and the UK, however, there is no extensive study on the right to privacy in cyberspace pertaining to cybersecurity and data protection in India. The researcher undertakes to do a comprehensive study on the right to privacy in cyberspace and also certain very important concerns such as cybersecurity and data protection.

This research aims at exploring various threats posed by the cyberspace, and thereafter, to study and identify the policies and legal framework in place in order to deal with these threats. This research further aims to critically analyse the current legal system which provides cyber security. This research shall also point out the inadequacies, gaps and loopholes in the present system and will suggest robust tools to deal with them.

The importance of the present research lies in two areas, one that it delineates and analyses the current legal framework in respect of data protection and cyber security and secondly, that it studies the inadequacies, gaps and loopholes in the present system and gives several suggestions and recommendations based on extensive research.

The present research is also significant in the sense that it shall give a model provision in the Constitution of India containing the provisions pertaining to the Fundamental right to privacy and the restrictions thereon and also listing the various facets of the right to privacy that have been afforded protection.

RESEARCH METHODOLOGY

The research methodology to be adopted by the researcher shall be doctrinal as well as empirical. The doctrinal research shall focus on the concept of privacy in cyberspace, its genesis, the legal framework in multiple jurisdictions. As a part of the doctrinal research, the researcher shall use the secondary data provided by various governmental institutions such as the National Crime Records Bureau in India amongst others. The research study will also be descriptive in nature wherein the existing legal position pertaining to cyber crimes and data protection shall be analysed and comparative study with various countries shall be done. The comparative study will be largely based on secondary data including reports by government bodies of various countries. The Doctrinal Research so undertaken will be complemented by empirical research.

Since the present study aims at studying the inadequacies in the current legal framework pertaining to privacy in cyberspace, cybersecurity and data protection, the same has been done by the researcher by way of non-doctrinal research. The researcher will be conducting primary research to test the hypothesis and in order to achieve the research objectives. Due to time and budgetary constraints the empirical research shall be limited to Delhi NCR. The researcher shall study the gaps/inadequacies in the existing system of combating cyber crimes and providing data privacy through both primary and secondary research. The researcher will conduct personal interviews of various officials closely dealing with cyber crimes and entrusted with the protection of data such as the Police Officials including the Investigating Officers, Judicial Officers and various legal luminaries. This is done with a view to understand the current legal position and the inadequacies, so that the researcher may give meaningful suggestions and recommendations. Primary Research shall also be conducted by getting questionnaire filled from the officials dealing with cyber crimes and entrusted with the protection of data as mentioned above and also from the victims of cyber crimes to further analyse the subject of the study.

Doctrinal Research

As part of doctrinal research, the researcher shall study the concept and genesis of the right to privacy in cyberspace in detail and shall also survey the current legal framework for cybersecurity and data protection so as to develop a clear understanding of the technicality and practicality of the concept. The researcher shall also conduct a comparative study of the right to privacy in India and in other jurisdictions of the world and reasons for success/failure/effectiveness of the concept in different legal systems.

For this purpose, the researcher shall extensively go through the various books, research articles, bare legal provisions, parliamentary debates, practice directions issued by various High Court/District Courts, various judgments of Supreme Court & different High Courts. The researcher shall, inter-alia, use the secondary data & reports published by Government/Non-Govt. Organisations such as National Crime Records Bureau (NCRB), National Judicial Data Grid (NJDG), National State Legal Service Authority, State Legal Service Authorities, Law Commission of India, Supreme Court of India, Various High Courts, Ministry of Law & Justice, Government Committees, etc.

Empirical Research

As part of the empirical research, the researcher shall conduct personal interviews of various jurists having vast experience in the subject, and of the persons such as Secretaries, District Legal Services Authority, Judicial Officers, Private Counsels, Public Prosecutors, Legal Aid Counsels including Jail Visiting Advocates, Police Officials including Investigating Officers. The empirical research shall be kept limited to Delhi region. The target Group shall be Officials of the Cyber Crime Cell, Judicial Officers, Legal Luminaries and Jurists.

Data shall be collected through personal interviews and questionnaires. The insights gained into the concept through doctrinal research as well as aforesaid in-depth/unstructured personal interviews, will help the researcher in assessing & narrowing down various aspects of the study like inadequacies in the current system.

Data obtained through doctrinal research shall be analysed extensively through deductive approach. Further, the data collected through non-doctrinal research shall be arranged in a systematic way & wherever possible, shall be tabulated & the same shall be analysed using appropriate statistical tools so as to achieve the desired objective as well as to test the formulated hypotheses.

SCOPE AND LIMITATION OF THE STUDY

The research shall encompass within itself the use of both the primary as well as the secondary sources. Due to time and budgetary constraints, the present research shall be kept limited to the Delhi NCR region. However, the target group will be wide and the researcher while employing the techniques of questionnaires and personal interviews will collect data from Secretaries, District Legal Services Authority, Judicial Officers, Private Counsels, Public Prosecutors, Legal Aid Counsels including Jail Visiting Advocates, Police Officials including Investigating Officers. Researcher's recommendations shall be based on primary research duly complemented by the use of secondary data.

REVIEW OF LITERATURE

Rishika Taneja and Sidhant Kumar in their book titled as, 'Privacy Law: Principles, Injunctions and Compensation' published by the Eastern Book Company in the year 2014, have surveyed the law relating to privacy in its various dimensions and in the context of several emerging situations. The authors have referred to the relevant case laws wherever required. The authors have discussed the contours of the right to privacy both under public law and under private law, meaning thereby, they have discussed the right to privacy as a fundamental right as well as the right to privacy as a tort. The book undertakes a critical appraisal of the existing framework of laws. What makes their work unique is the part where the authors have discussed the balancing of several rights vis-a-vis the right to privacy.

Gaurav Goyal and Ravinder Kumar in their book titled as, 'The Right to Privacy in India: Concept and Evolution', published by Partridge India in the year 2016, have dealt with the meaning, evolution and various constitutional aspects of the right to privacy. The authors have traced privacy from the times of Ramayana and Mahabharata to the modern times. Besides studying the right to privacy as prevailing in India, the authors have also undertaken a comparative analysis of the right to privacy in India, the United States of America and the United Kingdom. The authors have also studies the right of privacy in the light of various other rights and more particularly the right to information.

Rahul Mattan in his book titled as, 'Privacy 3.0: Unlocking our Data-Driven Future', published by Harper Collins publishers India in the year 2018, has dealt with the changing notions of privacy. He has divided his work in three parts, Privacy 1.0, Privacy 2.0 and Privacy 3.0 and has also enunciated the changes in the understanding of privacy through

various times. The author has identified the central issue which is data protection. Thus, the author has traced the evolution of the right to privacy through various times and stages and has also discussed the future course in regard to the protection of right to privacy.

Caroline Kennedy and Ellen Alderman in their book titled as 'The Right to Privacy', published by Knopf in the year 1995, examine the privacy issues in America by focussing on real-life incidents. The authors have dealt with the state of the right of privacy in modern day America with the help of several case studies showing the intrusion on the peaceful enjoyment of right to privacy of the individuals by government, businesses, the news media, and their own neighbours. The authors have examined the case studies very thoroughly and have delineated the privacy issues pertaining to the case. The authors have also discussed the competing rights of other persons, such as the freedom of press, as also the ethical issues involved in the case studies. The authors have particularly focused on the privacy concerns faced by women.

R.K. Dubey and Ajay Verma in their book titled as 'Data Protection and Privacy Implementation: India Perspective', published independently in the year 2019 have discussed the laws relating to data protection and privacy implementation in various jurisdictions with special reference to India. They have also given an insight into the recent global developments in that area including the General Data Protection Regulations (GDPR) by European Union, California Consumer Protection Act (CCPA) in the USA, etc. The authors have also studied the Justice Srikrishna Committee report on the Personal Data Protection Bill. Along with this, they have discussed several provisions relating to the India's Personal Data Protection Bill. It details steps for a data privacy implementation covering.

Pavan Duggal, an advocate by profession and a leading expert in cyber law and mobile law, in his book titled as 'Cyber Security Law', published independently in the year 2019, has discussed the importance and significance of a robust cyber security law. He has further discussed the impact of breaches in cyber security on the sovereignty of the nation as also the national security. The author has delineated the emergence of the cyber security law as a discipline. The author has also discussed the connected legal, policy and regulatory issues in relation to the cybersecurity.

Pavan Duggal in his book titled as 'Blockchain Law: A Primer', published independently in the year 2019, has given a brief view of the emerging legal landscape pertaining to blockchain law. The author has studied the various legal, policy and regulatory

issues involved in the widespread adoption of blockchain technology. This Book seeks to look at the legalities concerning Blockchains in various areas of human activities, analyse the liability of Blockchain service providers, and other issues like data privacy and intellectual property rights.

Pavan Duggal in his book titled as 'Cyber Security Law: Thoughts on IoT, AI & Blockchain', published independently in the year 2019, has discussed the impact of cybersecurity in the development, growth and subsequent commercial adoption of Internet of Things, Artificial Intelligence and blockchains. This Book seeks to analyse some of the important cyber security legal principles that need to be made as an integral component and part of the growth and further evolution of emerging technologies like Internet of Things, Artificial Intelligence and Blockchains. The author while admitting that much work needs to be done in this area and very limited information is available in the public domain at the current times, has tried to encapsulate the significant and complicated legal principles impacting the Internet of Things, Artificial Intelligence and Blockchains.

Pavan Duggal in his book titled as 'Indian National Cyber Security Policy-A legal Analysis', published independently in the year 2015, has studied the National Cyber Security Policy, 2015 in detail and its effect in the protection and preservation of cyber security in India. The book discusses both the highlights of the policy as well as the drawbacks concerning the said policy. This Book further elaborates on the various legal challenges facing the ever important issue of regulation of cyber criminal activities in the electronic ecosystem in India.

Pavan Duggal in his book titled as 'Whatsapp & Indian Cyberlaw', published independently in the year 2015, has analysed the legality of the use of the WhatsApp in India and role of this app in the increasing cyber crimes and cyber terrorism by various vested elements. It also seeks to examine other challenges pertaining to use of WhatsApp by various actors as the mobile messaging platform. This book helps the readers to understand the legal ramifications of using mobile messaging applications like WhatsApp.

Pavan Duggal in his book titled as 'Cyberlaw, Free Speech & Privacy', published independently in the year 2015 has examined role and significance of free speech and expression on the Internet and what are the various legal mechanisms pertaining to free speech especially in the context of countries like India. The author has discussed the impact of telecommunications and broadcasting law on Internet regulation worldwide and also

specifically in India. The Book also thereafter examines the issues pertaining to the right to privacy and how it is dealt with in different jurisdictions and also in India.

Raghu Santanam, M. Sethumadhavan and Mohit Virendra in their book titled as 'Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspective', published by Information Science Reference in 2011, have analysed the recent developments in cyber security, crime, and forensics. The authors have discussed the cyber crime in detail with specific reference to case studies, including, the UID Project, outsourcing, BPO risk & security, the emergency response of the Mumbai terror attacks. The authors have also examined the issues involved in copyright and cyberspace. The authors have also discussed the technological issues concerning cyber security. The authors have further delineated the various methods and algorithms for improving cyber security. The authors have reviewed and analysed the techniques and approaches that secure information at its fundamental level. This books conducts a multi-disciplinary research needed to address the wide range of challenges facing us today in the Information Age. In this book, the authors have taken the initial steps to define and explore the underlying issues related to cyber security and cyber crime.

Roger W. Smith in his book titled as 'Cyber Crime- A clear and Present Danger: The CEO's Guide to Cyber Security', published in the year 2014, has very deeply illustrated the theft of information online by cybercriminals which is resulting in loss of lakhs of rupees every year. This book also provides various measures to be adopted by companies and individual alike to defend their personal information.

Shrikant Ardhapurkar, Tanu Srivastava et. al. in their article titled as 'Privacy and Data Protection in Cyberspace in Indian Environment' published in International Journal of Engineering Science and Technology, Vol. 2 No. 5 in the year 2010, have dealt with the privacy issues in Indian perspective with respect to challenges in three different dimensions which are Legal, Technical and Political domain and have proposed a Framework for data collection, data storage etc. for ensuring better privacy in cyber space and have comprehensively dealt with major challenges of privacy in cyber space by referring to provisions of Information Technology (Amendment) Act 2008.

Dr. Deepti Khubalkar in her Article titled as 'Data Protection and Privacy in Cyberspace: National and International perspective' published in Psychology and Educational Journal, Vol. 57 No. 9 in the year 2020 has dealt with data protection and data privacy issues in India including the compliance which is becoming utmost important especially during

Covid-19 pandemic and highlights the importance of legal framework in India to provide protection for consumers and privacy considerations for organisations with respect to electronic data. She has also analysed the present legal system for protection to data privacy in India and various bills relating to data protection and privacy in India.

Mayur Choudhary and Peri Pratima in their Research paper titled as 'Privacy and Cyberspace in India: A critical analysis of Justice Srikrishna Committee Report and The Personal Data Protection Bill, 2018' published in International Journal of Law, Management and Humanities, Vol. 4, No. 3 have dealt with privacy issues on various Social Media Platforms like facebook, instagram, snapchat are seeing ever increasing user base and have pointed out the lacunae in the present laws and stresses the need for robust laws in line with the landmark judgement of Supreme Court which recognised Right to privacy as a fundamental right flowing from Article 21 of the Constitution of India and have also analysed Justice B.N. Srikrishna Committee report on Data Protection Law and the Personal Data Protection Bill, 2018 and have made comparisons with Europe's General Data Protection Regulation and India's take away from it.

Shiv Shankar Singh in his article titled as 'Privacy and Data Protection in India: A Critical Assessment' published in Journal of the Indian Law Institute, Vol. 53, No. 4 in the year 2011 deals with the right to privacy and data protection in the Indian Perspective and addresses the inherent conflict between right to privacy and data protection and deals with different arenas of data protection including financial details, health information, business proposals, intellectual property and sensitive data.

Mark J Taylor and Jeannie Marie Paterson in their article titled as 'Protecting Privacy in India: The roles of consent and fairness in data protection' published in The Indian Journal of Law and Technology, Vol. 16, No. 1 in the year 2020 wherein they have analysed the Indian Personal Data Protection Bill 2019 which provides a unique approach to balancing the elements of individual consent and fairness-based limitations that are used in data protection regimes in other parts of the world.

TENTATIVE CHAPTERIZATION

Chapter 1: Introduction

In this Chapter, the researcher will cover the basic introduction to the study, along with an overview of the concept of privacy and cyberspace and the right to privacy. The

researcher has further covered the review of literature and the statement of problem. The researcher has further enunciated the objectives of the study, its hypothesis, the significance of the study as also the research methodology adopted to meet the research objectives and finally the structure of the thesis.

Chapter 2: Concept and Genesis of Privacy and Cyberspace

In this Chapter, the researcher will pen down meaning and concept of privacy as also the typology of privacy while discussing various contours of the right of privacy as recognised in India. The researcher will also analyse the historical origins of the concept of privacy in India and shall also deal with a brief history of evolution of concept in foreign countries.

Chapter 3: Multi-Jurisdictional Analysis in respect of Right to Privacy, Cybersecurity and Data Protection

In this Chapter, the researcher will be doing a comparative analysis of the provisions in respect of protection of Right to Privacy, providing cyber security and combating cyber attacks, as also the strategies adopted and laws enacted in order to protect the data of the individuals in various countries of the world.

Chapter 4: Legal Framework in respect of Right to Privacy, Cybersecurity and Data Protection

In this Chapter, the researcher will be conducting a descriptive research of the various statutory provisions, constitutional guarantees, Judicial Precedents and Governmental Policies in respect of Right to Privacy, Cybersecurity and Data Protection. The researcher will also deal with the various regulatory authorities entrusted with the work of combating cyber crime and protection of data and their roles.

Chapter 5: Analysis of Data

In this chapter, the researcher will analyse the data collected from personal interviews and questionnaires filled by various officials closely dealing with cyber crimes and entrusted with the protection of data in practice. This data will be collected with the objective of understanding the shortcomings/ inadequacies in the current legal framework pertaining to Right to Privacy in Cyberspace.

Chapter 6: Conclusion and Recommendations

This Chapter has been devoted to detailed critical appraisal, conclusion and give various recommendations and suggestions.

BIBLIOGRAPHY

BOOKS

1. Rishika Taneja and Sidhant Kumar, PRIVACY LAW: PRINCIPLES, INJUNCTIONS AND COMPENSATION (2014).
2. Gaurav Goyal and Ravinder Kumar, THE RIGHT TO PRIVACY IN INDIA: CONCEPT AND EVOLUTION (2016).
3. Rahul Mattan, PRIVACY 3.0: UNLOCKING OUR DATA-DRIVEN FUTURE (2018).
4. Caroline Kennedy and Ellen Alderman, THE RIGHT TO PRIVACY (1995).
5. R.K. Dubey and Ajay Verma, DATA PROTECTION AND PRIVACY IMPLEMENTATION: INDIA PERSPECTIVE (2019).
6. Pavan Duggal, CYBER SECURITY LAW (2019).
7. Pavan Duggal, BLOCKCHAIN LAW: A PRIMER (2019).
8. Pavan Duggal, CYBER SECURITY LAW: THOUGHTS ON IOT, AI & BLOCKCHAIN (2019).
9. Pavan Duggal, INDIAN NATIONAL CYBER SECURITY POLICY-A LEGAL ANALYSIS (2015).
10. Pavan Duggal, WHATSAPP & INDIAN CYBERLAW (2015).
11. Pavan Duggal, CYBERLAW, FREE SPEECH & PRIVACY (2015).
12. Raghu Santanam, M. Sethumadhavan and Mohit Virendra, CYBER SECURITY, CYBER CRIME AND CYBER FORENSICS: APPLICATIONS AND PERSPECTIVE (2011).
13. Roger W. Smith, CYBER CRIME: A CLEAR AND PRESENT DANGER: THE CEO'S GUIDE TO CYBER SECURITY (2014).
14. Durga Das Basu, COMMENTARY ON THE CONSTITUTION OF INDIA (2015).
15. MP Jain, INDIAN CONSTITUTIONAL LAW (2014).

INTERNATIONAL DOCUMENTS REFERRED

1. Universal Declaration of Human Rights.
2. International Covenant on Civil and Political Rights.
3. Report of the Office of the United Nations High Commissioner for Human Rights No. A/HRC/27/37 dated June 30, 2014.

WEB LINKS REFERRED:

1. https://www.ijlmh.com/paper/right-to-privacy-and-data-defence/#.
2. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=6272&context=libphilprac.
3. https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/amp/.
4. https://ohrh.law.ox.ac.uk/defining-the-right-to-privacy-in-india-in-light-of-justice-ks-puttaswamy-anr-v-union-of-india-2017.
5. https://economictimes.indiatimes.com/protected-systems-and-networks/articleshow/43196757.cms.
6. https://economictimes.indiatimes.com/tech/technology/govt-withdraws-data-protection-bill-2021/articleshow/93334281.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
7. https://etc.bdir.in/quotes/view/MjY4NDQ=.
8. https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc.
9. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.1_1.pdf.
10. https://www.livemint.com/Politics/SvXJcx6Rfn3LuLjbKKj52M/EPFO-discontinues-services-through-CSC-pending-vulnerabilit.html.
11. https://www.livelaw.in/news-updates/delhi-high-court-right-to-be-forgotten-google-indian-kanoon-to-block-judgment-of-american-citizen-ndps-174655?infinitescroll=1.
12. https://www.ijlmh.com/paper/privacy-and-cyberspace-in-india-a-critical-analysis-of-justice-srikrishna-committee-report-and-the-personal-data-protection-bill-2018/.
13. https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf.
14. https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.
15. https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf.